GDPR 與圖書館

魏令芳與李明錦

歐盟的通用資料保護法規（General Data Protection Regulation，簡稱GDPR）已於2018年5月25日開始生效，當然引起了許多與歐盟有關組織的緊張，FACEBOOK、Google或是Microsoft這些公司也要重新調整有關資料的蒐集、保存或保護方式。據天下雜誌的報導指出，台灣和歐盟的經貿關係，雖無如北美緊密，但各行各業相關組織只要沾到歐盟的邊，就立即受到GDPR規範。George Washington University的法律教授Daniel Solve指出：「這是我們這一代影響最深遠的隱私法（the most profound privacy law of our generation）」，網路上稱為史上最嚴苛的資料保護法，遠遠超過當前其他地區和大多數國家的現行個人資料保護法範圍。這些層面對於學校而言，如相關交換計畫、國外研習、訪問學人、位於他國的校區與研究圖書館，與歐盟相關的都納於此範圍內。

圖書館的論壇也免不了開始談論，畢竟圖書館也屬於資料蒐集與保存單位之一，論壇上的同儕詢問的標題是「GDPR與圖書館網站」，詢問其他圖書館可有去修改圖書館網站或數位平台以符合歐盟個人資料保護條例，其中來自VCU Libraries的Erin White指出，他們學校的IT群建立一個網頁說明蒐集個資相關資訊，另一位同儕則指出學校採購了OneTrust作為因應GDPR的解決方案，雖然熟悉度還是朦朦朧朧，然White指出這是一個可以提高讀者資料保護察覺度的機會。

圖書館界的相關訊息，如IFLA於2017年出版了*Briefing: Impact of the General Data Protection Regulation 2018*簡報資料，提醒圖書館須瞭解可能適用於圖書館的特定法律豁免。美國的圖書館同儕都希望LITA或是Code4Lib能多舉辦一些討論讓他們深入瞭解GDPR對美國圖書館的影響，美國研究圖書館學會ARL也於2018年5月上載*The General Data Protection Regulation: What Does It Mean for Libraries Worldwide?* 提供圖書館認識GDPR，持續會追蹤報導相關訊息。英國圖書資訊專業學會CILIP也製作一份指引提供圖書館專業人員認識與因應GDPR，並瞭解圖書館如何保管與處理個人資料，例如需不需要重新發信跟讀者做確認，採用雲端服務或使用圖書館系統時需如何跟廠商協談資料處理問題，圖書館的讀者資料可以保留多久，多久後進行清除？Princh畫了個圖讓我們熟悉GDPR，我們就跟著轉一轉走一回吧！

1. 認識GDPR

General Data Protection Regulation，簡稱GDPR，中文翻譯有「通用資料保護法規」、「通用數據保護條例」、「一般數據保護條例」、「數據資料保護條例」或是「一般資料保護規範」。此法規取代了數據保護指令95/46 / EC，目的是提供個人更多對於個人資料的控制。歐盟此舉是在保護和授權所有歐盟公民的數據隱私。陳育晟引自《經濟學人》最新報導於遠見雜誌上指出，此法規與以往最大區別是企業要民眾同意接受收集、處理個資須更明確，不能空泛表示「你的個資會被用來改善我們的服務」。民眾可要求蒐集單位出示個資複本，並要求修改或刪除儲存在企業內的個人資料。

其次，各大企業需要指派個資保護長（Data Protection Officer，簡稱DPO），且企業若違法，他們會在72小時內舉報。違法的企業最重可罰2,000萬歐元或當年全球總收入的4%（取其重）。要留意的是受罰的對象也有資料的控制者（Data Controller）與協助進行資料儲存或傳輸的資料處理者（Data Processor）。

ARL指出館員們可以追縱的資料來源如下：

- EU's GDPR Information Portal
- Library of Congress, "Online Privacy Law: European Union"
- LIBER, Webinar Video: "GDPR & What It Means for Researchers"

EDUCAUSE也重點指出獲取GDPR相關參考資料羅列如下，需要概覽可至AACRAO、ERGDPR.org、UCISA網站參考。

- GDPR 簡介，3 月 9 日 Elive！網絡研討會，錄製和幻燈片現已推出。
- JISC GDPR 於 2017 年 12 月會議錄音，提供這些變更的影響以及如何規劃和實施整個組織內的變更提供實用建議。
- EDUCAUSE 2017 在 11 月 2 日星期四舉行了新的歐盟一般數據保護條例：IT 專家需要了解的內容。

2. 識別圖書館處理資料

圖書館主要是向讀者提供服務，因此可能蒐集個人資料，個人資料被定義為"與識別或可識別的自然人有關的任何資訊"，因此可以是基本身份資料，如姓名、電話號碼、地址等或是基本的網路識別資訊，如電子郵件地址、cookies、IP地址，或者提供與物理，生理，遺傳有關的更具體資訊，這個人的精神，經濟，文化或社會身份。

圖書館可以從目的活動取得讀者資料，完成後，可以決定哪些資料包含個人資料，但別忘記了內部處理的資料，同時也包括由第三方處理的外部資料，如雲端解決方案和供應商所處理的資料，任何足以影響讀者個人資料洩露的情況，圖書館都需負責。圖書館檢視透過活動收集和處理的所有資料，是製定一個符合GDPR標準行動計劃的好起點。

2018年最新54卷3期的*Library Technology Reports*剛好談的是Privacy and Security Online: Best Practices for Cybersecurity，2016年52卷4期則是Privacy and Security for Library Systems，都是圖書館於此的相關議題，有興趣的同道可以持續深入閱讀。

3. 界定圖書館如何處理資料

經活動收集的資料及其來源，即可確定需要這些資料的原因以及為什麼它對圖書館活動的用處，決定圖書館實際需要儲存多久。為證明符合規定，圖書館必須更

新資料保護政策，並牢記有關個人資料處理原則，最重要的是資料主體的權利。讀者有訪問權、修改權利、刪除權利、限制權利、數據可移植性權利與反對權利。因此，無論何時收集了個人資料，都必須確保獲得使用該資料的同意，同時確保所有圖書館政策（隱私政策，條款和條件政策，Cookie政策等）都是為方便讀者使用。

4. 使用適當的評估方式

再來是於圖書館內部實施確定的變更，"控制者應實施適當的技術和組織措施，以確保在默認情況下，只處理每個特定處理目的所需個人資料。此階段目標是針對收集的資料執行保護規則。

鑑於網絡犯罪不斷增加，GDPR促使組織有必要製定一些程序來預防、監控、檢測和報告任何攻擊或安全漏洞。採取一些技術措施和培訓人員來關注這個問題是很重要的，依據新規定，一如其他收集資料機構，於72小時內回報違規行為並通知讀者。

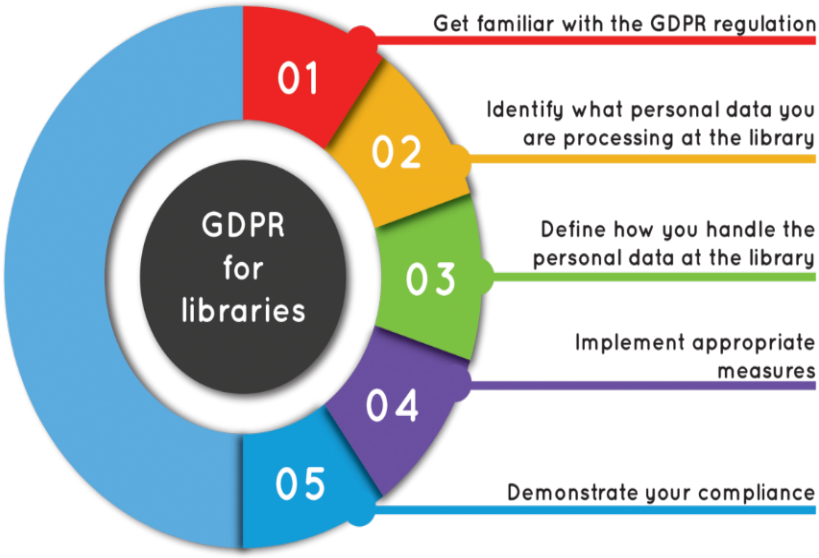
5. 展示你的使用

制定相關政策後是記錄流程並解釋活動隱私和安全方法的時候了。準備審核和希望訪問，糾正，刪除或移動資料的讀者。由於圖書館是處理資料的公共機構，因此需要指定資料保護員（DPO），其任務是成為監督機構與控制者和處理者之間的聯繫。最後將GDPR法規視為圖書館一項持續活動，重要的是瞭解圖書館發生的情況並保存日誌以準備好報告任何安全漏洞。

當然我們也閱讀到網路上OCLC、EBSCO與SirSiDynix這些與圖書館有關的組織及系統廠商對於DGPR的聲明。以OCLC來說，OCLC指出他們不銷售資料或是彙整多個來源資料，通常他們會將其資料匿名或偽匿名作為標準資料處理流程的一部份。他們也列出一些網路資料提供位於歐盟的圖書館或是收集有關歐盟個人資料的圖書館一些建立因應GDPR計畫的資源：

- 主要的 EUGDPR 網站
- 歐盟 Article 29 Working Party 資源
- 英國 The UK Information Commissioner's Office Guide to the GDPR
- The International Association of Privacy Professionals (IAPP) GDPR Resource Center

英國的Josephine Bailey於University of Sheffield完成的碩士論文，剛好針對英國圖書館調查有關因應GDPR的現況與看法，基本上回答了一個問題，就其所調查對象，圖書館準備好因應GDPR了嗎？基本上是正面的，圖書館意識到需要學習更多，需要依靠外部組織提供一些相關政策與訓練等，而且也已察覺到如上面所說明的隱私資料的管理與其流程一些資料保護事項。



資料來源：https://princh.com/gdpr-compliance-for-libraries-5-general-aspects-that-you-need-to-cover/

參考資料：

1. 王琍瑩 (2018)。歐盟高規格 GDPR 數據保護法上路，AI 新創該如何應對？上網日期：2018年5月24日。網址：https://www.cw.com.tw/article/article.action?id=5090080 。
2. 吳均龐 (2018)。【吳均龐專欄】為什麼你該擔心GDPR風暴？。上網日期：2018年5月24日。網址：https://www.cw.com.tw/article/article.action?id=5090085。
3. 陳育晟 (2018)。史上最嚴資料保護令 GDPR確定5月25日上路。上網日期：2018年5月24日。網址：https://www.gvm.com.tw/article.html?id=44159。
4. Bailey, Josephine. (2018). Data Protection in UK Library and Information Services: Are We Ready for GDPR? *Legal Information Management*, 18(1), 28-34.
5. Breeding, Marshall. (2016). Issues and Technologies Related to Privacy and Security. *Library Technology Reports*, 52(4), 5-35.
6. CILIP. (2018). Guide to GDPR. Retrieved from https://www.cilip.org.uk/page/gdpr
7. EDUCAUSE (2018). EU General Data Protection Regulation (GDPR). Retrieved from https://library.educause.edu/topics/policy-and-law/eu-general-data-protection-regulation-gdpr
8. Gilliland, Anne. (2018). The General Data Protection Regulation: What Does It Mean for Libraries Worldwide? Retrieved from http://www.arl.org/component/content/article/6/4543
9. Hennig, Nicole. (2018). Privacy and Security Online: Best Practices for Cybersecurity. *Library Technology Reports*, 54(3), 5-33.
10. Presas, Julie. (2018). GDPR: What does it mean for OCLC and your library? Retrieved from http://www.oclc.org/blog/main/gdpr-what-does-it-mean-for-oclc-and-your-library/
11. Princh. (2018). GDPR compliance for libraries – 5 general aspects that you need to cover. Retrieved from https://princh.com/gdpr-compliance-for-libraries-5-general-aspects-that-you-need-to-cover/
12. Solove, Daniel. (2018). Why I Love the GDPR: 10 Reasons. Retrieved from https://teachprivacy.com/why-i-love-the-gdpr/
13. White, Benjamin. (2017). Briefing: Impact of the General Data Protection Regulation 2018. Retrieved from

https://www.ifla.org/files/assets/clm/publications/briefing_general_data_protection_regulation_2018.pdf

聯絡資訊：

魏令芳
東吳大學圖書館讀者服務組編纂
weilf@scu.edu.tw

李明錦
國立臺灣大學醫學圖書館主任
tracy@ntu.edu.tw